

FILED _____ ENTERED _____
LOGGED _____ RECEIVED _____

OCT 17 2018

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
DEPUTY
BY _____

**IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
THE APPLE ID(s) linked to:**

IMEI 356572082018670, and

IMEI 353841087910253,

**WHICH ARE STORED AT PREMISES
CONTROLLED BY APPLE, INC.**

18 - 2691 - ADC

Case No. _____

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, James J. Jenkins, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am submitting this Affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed International Mobile Equipment Identities ("IMEI"), which are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described below and in Attachments A and B.

2. Your affiant is a Special Agent with the U.S. Department of State, Diplomatic Security Service (DSS), and has been employed by the Department of State since September 2011. Your affiant is currently assigned to Homeland Security Investigations' (HSI) Document

Handwritten signature/initials

b) **IMEI 353841087910253².**

For the reasons set forth below, your affiant submits that there is probable cause to believe that the iCloud accounts associated with these APPLE IDs are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

PROBABLE CAUSE

Summary Of Investigation

6. For more than one year, the Department of State Diplomatic Security Service (“DSS”), Homeland Security Investigations (“HSI”), and the U.S. Department of Labor – Office of Inspector General, Office of Investigations – Labor Racketeering and Fraud (“OILRF”) have been investigating **Asher SHARVIT (“A. SHARVIT”)**, **Rona ZHFANI (“ZHFANI”)**, and **Oren Sharvit (“O. SHARVIT”)** (collectively referred to as the “Defendants”), and other co-conspirators. Your affiant and other federal agents have obtained information from subpoenas, searches pursuant to the border inspection authority of the Department of Homeland Security (DHS), government records, search warrants, consent searches, interviews, surveillance, and other investigative means.

7. Based on the investigation to date, your affiant and other federal agents have obtained evidence that at various times during the period in or about 2012 to in or about 2017, **A. SHARVIT, O. SHARVIT, and ZHFANI** have owned, controlled, operated, worked for, and/or

² An iPhone with this IMEI was seized from Asher SHARVIT by DHS law enforcement officers. The iPhone’s SIM card is associated to the telephone number 443-949-6596

otherwise been affiliated with the following entities: Unlimited Treasures, Inc., Unlimited 13 Corp., Deja Vu Cosmetics, and others (collectively “Unlimited” or “Defendants’ Companies.”).³ The Defendants’ Companies leased or operated kiosks and stores in New York, Virginia, Maryland, and Delaware. The Defendants’ Companies often used the trade names Deja Vu and BioXage.

8. Your affiant submits that the evidence set forth herein shows that the Defendants and their co-conspirators (1) recruited foreign citizens to travel to the United States and work as employees in the Defendants’ Companies; (2) caused foreign citizens to apply for B1/B2 visitor visas and/or visa extensions,⁴ which did not permit employment in the United States; (3) paid foreign citizens in cash without reporting their employment to federal or state authorities, nor making proper payroll deductions; and (4) provided foreign citizens with travel reimbursements, and arranged their transportation and lodging in the United States, which facilitated the Defendants’ illegal use of foreign workers. The foreign workers were only paid on a commission basis, and the company paid no payroll taxes for foreign employees. Your affiant submits that

³ According to Maryland Department of Assessments and Taxation records, as of April 2010, **A. SHARVIT** was the registered agent for Unlimited Treasures and co-conspirator #4 was the registered agent of Unlimited 13 Corp, as of June 2015. Deja Vu Cosmetics is company that was based in Israel and Pennsylvania—co-conspirator #1 operated the Pennsylvania portion.

⁴ Individuals receiving B1/B2 visitor visas are supposed to be entering the United States for tourist and/or business purposes. While a visitor admitted in B1 status would be allowed to conduct business activities such as attending conferences, negotiating contracts, or consulting business associates, neither B1 nor B2 status confers authorization to work in the United States. At a Port of Entry, depending on their purpose of travel a foreign citizen is often admitted to the United States in either B1 (business) or B2 (tourist visitor) status.

this suggests that an object of the conspiracy was to increase the financial profits of Unlimited, which was controlled by the Defendants and their co-conspirators.

9. On or about June 25, 2018, this Court issued criminal complaints against the Defendants, finding that there was probable cause to believe that they had conspired to defraud the United States, in violation of 18 U.S.C. § 371.

10. On or about June 27, 2018, the Defendants were arrested as they entered the United States from Israel.

11. On or about June 27, 2018, three phones were seized from the Defendants by DHS law enforcement officers pursuant to the Border Search authority of the Department of Homeland Security.⁵

12. After she was arrested on June 27, 2018, **ZHFANI** told federal agents that she had helped out but had not worked at Unlimited; that **A. SHARVIT** sold his company a long, long time ago, and that Eyal Chertoff was the person to whom the business was sold. **ZHFANI** also claimed that maybe someone else had used her phone to send WhatsApp messages.

13. On or about July 10, 2018, the grand jury returned an Indictment against the Defendants, charging them multiple criminal offenses, in violation of 18 U.S.C. §§ 371, 1546(a); and 8 U.S.C. §§ 1324(a)(1)(A)(iv), 1324(a)(3), 1324(a)(1)(iii).⁶

14. On or about August 21, 2018, the grand jury returned a Superseding Indictment, which added obstruction of justice charges against **A. SHARVIT** and **O. SHARVIT**, in

⁶ Mordehay (aka Moti) FOOX, Eyal CHERTOFF, and Esti MAZOR are also associated with Unlimited.

violation of 18 U.S.C. §§ 1512, 1519. As part of the investigation, federal agents have uncovered evidence that in or about February 2017, the **A. SHARVIT, O. SHARVIT** and some of their co-conspirators caused and/or aided and abetted the destruction of documents, records, and tangible objects containing evidence of the crimes described herein, and corruptly persuaded others to destroy documents and records. Your affiant has also uncovered electronic evidence to support the obstruction of justice charges, including a voicemail left for co-conspirator #1⁷ and a receipt for shredding services sent to **A. SHARVIT** and co-conspirator #1 via WhatsApp.

Prior Search Warrants

15. Federal agents have previously sought and obtained search warrants for email accounts associated with the crimes under investigation as well as an iPhone 7 seized on or about July 27, 2017, from co-conspirator #1. *See* 17-2555-JMC (Sept. 19, 2017); 18-458-JMC (Feb. 23, 2018). As detailed further herein, the electronic evidence to date has yielded extensive evidence about the conduct of the scheme, including voluminous WhatsApp⁸ messages.

16. As a result of the investigation to date, including the electronic evidence, as well as interviews of Unlimited employees, your affiant has evidence that the Defendants and their

⁷ Any co-conspirator identified herein by number is a person who was an employee or otherwise associated with the indicted defendants by has not himself/herself been indicted for the offenses described herein.

⁸ WhatsApp is a messaging application that can be used on mobile phones. WhatsApp allows for voice calls and exchanging text messages including in a group with multiple recipients. The Defendants, along with other co-conspirators, were members of a WhatsApp message group titled "management." This group included "Asher," "אורן," "רונה" and the first names of co-conspirators #1, 2, and 3. A native Hebrew speaker reviewed the names רונה and אורן and your affiant learned that they translate to "Rona" and "Oren." Your affiant believes Asher refers to **A. SHARVIT**, Rona refers to **ZHFANI**, and Oren refers to **O. SHARVIT** and WhatsApp messages from these names are so attributed in this affidavit.

co-conspirators used electronic messages to discuss the conspiracy and details related to recruiting, hiring, scheduling, paying, and housing foreign citizens. In particular, the WhatsApp messages make plain that the Defendants knowingly used foreign citizens as employees and sought to circumvent the immigration and employment laws of the United States.

17. On June 26, 2018, U.S. Magistrate Judge Kevin Fox (SDNY), authorized a search warrant for the residence of **A. SHARVIT** and **ZHFANI** in New York, NY. During the search, agents located numerous electronic items including laptop computers and cellular phones, which are still being reviewed. Among other items, agents also located a notebook in the residence that contained handwritten names of malls and first names that appeared to be schedules and what appear to be agenda notes for a meeting with employees. Among the electronic items seized by law enforcement were a cell phones that appeared to have been used in the past by **A. SHARVIT** and **ZHFANI**. These phones contained relevant evidence, including WhatsApp conversations related to Unlimited.

18. On September 4, 2018, U.S. Magistrate Judge Beth P. Gesner (D.MD), authorized the search of three iPhones obtained by DHS law enforcement officers pursuant to their border search and seizure authority. Based on consultations with law enforcement sources familiar with the operation of Apple iCloud and iPhones, your affiant understands that relevant WhatsApp communications can also reside within the iCloud accounts of **A. SHARVIT** and **RONA ZHFANI**, and that law enforcement may be able to access such evidence directly from the iCloud data despite being unable to presently access the iPhones of **A. SHARVIT** and **ZHFANI** due to password protection.

The Defendants' Companies Had Foreign Citizens Working At Malls And Other Retail Locations Ranging From Washington, D.C. Area To The New York Metropolitan Area

19. The federal investigation has revealed that the Defendants' Companies primarily leased retail space at shopping malls in Maryland and Delaware. Agents have spoken with multiple representatives at shopping malls in Maryland and Delaware. From these interviews and records obtained, agents know that the business locations were often leased using the business entities Unlimited or Deja Vu Cosmetics. The stores often identified themselves to the public under the names Deja Vu Cosmetics and BioXage. Certain members of the conspiracy, including **A. SHARVIT**, were also affiliated with another venture called Filicori Zecchini.⁹ Your affiant has obtained copies of leases with malls, which reflect that co-conspirators #1, #3, and #4 were signatories for Unlimited related leases.¹⁰

20. Based on a WhatsApp message that **A. SHARVIT** sent on or about December 30, 2015, your affiant submits that **A. SHARVIT** had broad managerial responsibilities and that the scope of the conspiracy's operations was quite broad. In the WhatsApp message, **A. SHARVIT** provided an update on the leases of the conspiracy at various locations, writing:

"Ok Guy's so!!!

We will have 33 people left+Tami and israel+maya and you too!!;)
So 37+2 that needs to arrive.

⁹ **A. SHARVIT** and other members of the conspiracy are/were involved in operating multiple retail coffee shops called Filicori Zecchini. The coffee shops are located in New York and Maryland. Federal agents have identified multiple current or former employees of Maryland-based Filicori Zecchini locations who are/were in the United States on visitor visas or on a visa waiver (which also prohibits employment). **A. SHARVIT** and others are believed to be investors in Filicori Zecchini locations.

¹⁰ This affidavit references co-conspirator #1, co-conspirator #2, co-conspirator #3, and co-conspirator #4. None of those four individuals are the named Defendants herein.

We will keep:

- *Mills1+2(Lease signed)
- *Fsk mall(lease signed)
- *Valley(lease signed)
- *Towson(lease signed)
- *Wheaton mal(signed)
- *christianna(signed)
- *Towson store(signed)
- *Christianna store (signed)
- *Roosevelt store(signed)
- *Whitemarch(moti)
- *Harford(jean mi please sign for one month at the rate we pay and tell her we might renew)
- *Pg Piazza(Please renew for one month and tell her at this rate we can not stay more for the moment)

Locations to close tommorow night:(5,jean mi please organize closings properly and make sure all products will be reused for the other locations)

Valley 2

Pg 2

Francey 2

Springfield

Annapolis

Mills 3

Yallaaaaa guy's we start the year with 13 locations!!!;)

Woujouuuuuuu!!!!!!!!!!!!!!”¹¹

¹¹ Based on context, geography, and information gathered during the investigation, your affiant believes “Mills” referred to Arundel Mills Mall, “Fsk mall” referred to Francis Scott Key Mall, “Valley” referred to Valley Mall, “Towson” referred to Towson Town Center, “Wheaton” referred to Westfield Wheaton, “Christianna [sic]” referred to Christiana Mall, “Roosevelt store” referred to a store operated in the Roosevelt Hotel in New York, “Whitemarch [sic]” referred to White Marsh Mall, “Harford” referred to Harford Mall, “Pg Piazza [sic]” referred to The Mall at

21. On or about December 20, 2015, **A. SHARVIT** was sent an e-mail entitled “List of Employees + Malls + Apartments.” The e-mail included a spreadsheet attachment entitled “Employees list DEC 2015.xlsx.” The “employees” tab contained the names of **O. SHARVIT** and **ZHFANI** as well as 50 first and last names and one first name. Hereinafter, those employees are identified by their initials (as are other individuals believed to be employees of the Defendants’ Companies).

22. The employee list did not contain dates of birth, thus making it difficult to identify and cross-reference employees to immigration records with certainty. Using other records and information obtained during this investigation, your affiant has been able to identify 10 employees on the list (O.P., S.Y., L.C., Y.E., E.S., M.G., R.Z., A.D., L.B.M., and A.A.) as foreign citizens present in the United States without work authorization. Your affiant has also been able to identify two employees, M.B. and H.C., as having legal authorization to work in the United States. Your affiant submits that based on the investigation and information detailed herein that there is probable cause to believe that the majority of these 51 employees lacked authorization to work in the United States and were therefore illegally employed.

23. On or about the same day, December 20, 2015, **A. SHARVIT** sent a WhatsApp message to the other Defendants and co-conspirators, which included the names of Mall locations, such as “Towson” or Pg Plaza” as well as hours, such as “(7h00 am-10h00pm)” or “(6h30-11hpm).” Under each location, **A. SHARVIT** listed certain Unlimited employees,

Prince Georges, “Springfield” referred to Springfield Town Center, and “Annapolis” referred to Westfield Annapolis.

typically using just their first names. Many of these first names match the full employee names emailed to **A. SHARVIT** on or about December 20, 2015.

Foreign Workers Were Recruited And Employed As Part Of The Conspiracy

24. Through records and interviews, your affiant and other federal agents have identified more than 40 foreign citizens who are believed to currently work or have worked at the Defendants' Companies and/or Filicori Zecchini. Based on information gathered, it appears that most Unlimited employees were foreign citizens and the majority of the foreign citizens entered the United States on visitor visas or under visa waivers. Your affiant and other federal agents have uncovered electronic evidence as well as information from other sources that has revealed that the Defendants and their co-conspirators actively sought out foreign citizens to work at Unlimited. In particular, your affiant and other federal agents have reviewed messages in either WhatsApp and/or emails in which **A. SHARVIT** and others communicated about the recruitment, transportation, and visa statuses of foreign citizens.

25. For example, your affiant located an email forwarded to co-conspirator #1 in or about April 2015. The email appears to have been initially sent by **A. SHARVIT** in which he wrote: "I was thinking yesterday of where we are standing and where we need to go...Also I wrote a plan that will direct us for the near future." Attached to the email was a Microsoft Word document that significantly included the following points:

- **"*The business is growing by: 1. Bring new employees by opening an efficient manpower office in Israel:**
Goals: bring as many employees as we can from Israel for our retail companies but also in the near future by selling them to other retail companies that will sell our products;" and

- “2. keep working with creation¹² and maybe start to work with another man power Israeli company.”

26. Several WhatsApp messages were similarly revealing. On or about June 1, 2015, co-conspirator #2 sent a WhatsApp message to the Defendants and other co-conspirators. The message contained an employment contract, which was signed by co-conspirator #2, and written in Hebrew with the title “Unlimited.”

27. A Hebrew speaker working at the U.S. Consulate in Tel Aviv translated the employment contract. According to the translation, Unlimited employees were: (i) required to work 5 ½ days per week; (ii) paid every two weeks based solely on their sales (a commission of 25-30%); (iii) provided with local travel arrangements upon their arrival at an airport in the United States; (iv) offered a 50% reimbursement of their airplane travel costs if they worked for Unlimited for three months and a complete reimbursement if they worked for six months; (v) offered advanced sales training at Unlimited’s office; (vi) provided with shared housing that included the first month free, and a weekly rent of \$135 thereafter; and (vii) offered access to vehicles for getting to work and/or use during their days off.

28. The name and Israeli identification number of O.P. are listed in the employment contract.¹³ Your affiant learned from U.S. government records that O.P. entered the United States on or about June 10, 2015 as a B-2 visitor, who was not authorized to work in the United States.

¹² Your affiant believes “creation” is a reference to the recruiting company used by the Defendants to locate potential workers in Israel.

¹³ Your affiant submits that the June 1, 2015 WhatsApp message and attached document demonstrate probable cause to believe that the foreign citizen entering into this agreement actually worked for Unlimited.

While in the United States, O.P. applied to extend his period of admission. He subsequently departed on or about January 12, 2016. On or about September 21, 2016, co-conspirator #2 sent WhatsApp messages (which your affiant used Google to translate) to the Defendants and other co-conspirators with a photograph of the boarding pass of O.P. and said that he would contact two co-conspirators for pick-up in Baltimore. The next day, O.P. re-entered the United States and was admitted on B-2 status.

29. On or about September 17, 2015, **A. SHARVIT** sent a WhatsApp message to other Defendants and co-conspirators containing the travel itinerary of S.Y. **A. SHARVIT** then sent instructions (which your affiant used Google to translate) to obtain a train ticket for S.Y. to travel from New York to Baltimore and asked that the ticket be sent to co-conspirator #2. On or about September 18, 2015, S.Y. entered the United States and was admitted on a B-2 visa as a visitor.¹⁴

Defendants' Companies Obtained Housing For Foreign Employees

30. Unlimited obtained housing for the foreign employees. Agents have identified Fallstaff Manor Apartments in the Pikesville area of Baltimore City ("Fallstaff") as a location where many foreign citizens who worked for Unlimited lived.¹⁵ Based on the investigation to

¹⁴ S.Y. subsequently sought an extension of her visitor visa, using a money order that your affiant has linked to Unlimited.

¹⁵ Your affiant also learned through records and information from a co-conspirator that Unlimited also housed workers at 3505 Clarks Lane, Baltimore, MD. According to Maryland property records, this property is owned in the name of 3505 Clarks Ln LLC. According to organization records from the State of Maryland, **A. SHARVIT**, was listed as an "authorized person" on the initial articles of organization for 3505 Clarks Ln LLC, though he has since been removed.

date, the Unlimited employees' housing at Fallstaff was arranged by upper-level members of the conspiracy. Agents interviewed a Fallstaff representative who said that between February 2013 and March 2017, A. SHARVIT and a co-conspirator rented approximately 13 different apartments. The Fallstaff representative advised that he/she believed the apartments were used to house employees of Unlimited Treasures.

31. Agents obtained leases and applications from Fallstaff Manor Apartments and found that there were approximately 13 apartments associated with Unlimited Treasures.

A. SHARVIT signed several of the apartment leases.

The Defendants Conspired To Assist Employees In Filing Fraudulent Visa Extensions

32. The federal investigation, as detailed herein, has revealed that the Defendants sought to influence and persuade foreign citizens to fraudulently enter the United States on visitor visas, and/or to file B-1/B-2 visa extensions with U.S. Citizenship and Immigration Services ("USCIS") that contained fraudulent information. In many cases, the Defendants' Companies paid fees to the immigration attorney who handled the visa extensions and later deducted the cost from employees' wages. The Unlimited employees would submit certain documents in their extension applications, including a Form I-539 (Application to Extend/Change Nonimmigrant Status) and supporting documentation. The Form I-539 contained the following question: "Have you, or any other person included in this application, been employed in the United States since last admitted or granted an extension or change of status?" The investigation has revealed numerous Unlimited employees who applied for visa extensions and fraudulently answered no on their Form I-539.

33. Your affiant has been able to link a number of I-539 filings to the Defendants' conspiracy through either the address used on the form and/or through photocopies of money

orders submitted as supporting documents to show that the applicant had access to funds to pay for their extended stay in the U.S.

34. Your affiant reviewed multiple I-539s filed by foreign citizens linked to Unlimited. Summary details of the applications are listed below. The applicants listed below listed Unlimited associated apartments as their address and/or used money orders linked to the conspiracy:

Name	Date signed	Linked address	Linked money order
R.Z.	07/08/2013	Yes	No
M.C.	10/10/2014	Yes	Yes
E.S.#2 ¹⁶	12/19/2014	Yes	Yes
L.C.	10/12/2015	Provided an address used by Defendants' Companies on other documents	No
E.S.	11/23/2015	No	Yes
Y.A.	12/22/2015	Yes	Yes
M.G.	1/7/2016	No	Yes
S.Y.	3/15/2016	No	Yes

¹⁶ Numbers after an individual's initials are to indicate they are a different person than the one previously identified herein with the same initials.

L.C.	5/24/2016 (second application)	Provided an address used by Defendants' Companies on other documents	Yes
Y.E.	5/24/2016	Provided an address used by Defendants' Companies on other documents	No
L.B.M.	6/3/2016	Yes	No
Y.B.	6/3/2016	Provided an address used by Defendants' Companies on other documents	Yes
D.S.	11/09/2016	No	Yes
A.B.	11/15/2016	No	Yes
N.B.A.	12/1/2016	No	Yes
A.A.#2	12/20/2016	No	Yes
M.G.#2	Undated, received by USCIS in 2016	No	Yes

35. Your affiant located messages indicating that the Defendants were aware of employees filing visa extensions and, in some cases, **A. SHARVIT** directed a co-conspirator to assist employees in the extension filings.

36. On or about April 11, 2016, **ZHFANI** sent a WhatsApp message to the Defendants and co-conspirators in Hebrew. Using Google Translate your affiant found that it said "I made a call to [First name of L.C.] and he starts working on extending the visa he will stay here." Your affiant believes that this likely refers L.C. and his preparation to file a Form I-539.

H2

37. On or about September 22, 2016, **A. SHARVIT** sent a WhatsApp group message in English to the other Defendants and co-conspirators, including **O. SHARVIT** and **ZHFANI**, directing co-conspirator #3 to make sure visa extensions were done at least a week before they were due and to make sure they were completed.

Each Of The Defendants Knowingly Joined The Conspiracy

38. The federal investigation has revealed that **A. SHARVIT** is one of the most senior members of the conspiracy. As detailed herein, **A. SHARVIT** was a manager of a wide-ranging conspiracy involving more than 50 individuals. The conspiracy recruited, hired, and paid foreign citizens as employees while knowing that many of the employees were present in the U.S. on visas that did not permit employment and in some cases, as detailed herein, facilitating or encouraging the employees to obtain visa extensions to remain in the United States in an immigration status that did not permit employment.

39. The investigation has revealed that the Defendants took actions consistent with employer-employee or manager-employee relationships. These behaviors included assigning employees to work locations, approving requests for leave, firing employees, and paying employees. In reviewing WhatsApp messages associated with this investigation, your affiant also located messages sent by **ZHFANI** and **O. SHARVIT** that appeared to be daily work assignments. These messages appear consistent with individuals exercising mid-level supervisory authority.

40. On or about December 22, 2015, **A. SHARVIT** sent a message in English to other Defendants and co-conspirators stating “[First name of M.S.] is going to get fired tonight,[first name of co-conspirator #3] please prepare her paycheck.” Your affiant believes that

the first name refers to M.S. According to U.S. government records, M.S. was present in the United States on M-1 (non-academic vocational training) visa status.

41. Your affiant discovered videos in the WhatsApp program on co-conspirators #1's phone that appear to depict work parties and/or meetings attended by Unlimited employees. These parties/meetings appear to have been designed to motivate and encourage the employees. During one video, **A. SHARVIT** and **O. SHARVIT** are featured prominently leading the group in song and celebration. Based on information provided to your affiant, it is your affiant's understanding that employees were paid at group meetings similar to these.

42. Your affiant has identified multiple WhatsApp messages that were sent or received by **A. SHARVIT**, **O. SHARVIT**, **ZHFANI**, and other members of the conspiracy that listed employees' first names, and appeared to list the amounts that they were to be paid for a particular pay period. Some messages specifically indicated they were "paychecks." Nevertheless, the investigation to date has revealed that most of the employees were not paid by checks from a bank or payroll company, but instead paid by cash, and without any required withholding under state and federal laws.

43. Your affiant found a message exchange in the WhatsApp message group used by the Defendants and other co-conspirators in which **O. SHARVIT** and a co-conspirator discussed not having enough cash to pay the "paycheck" of two employees and referenced having to wait for the envelopes to come back. Based on the investigation, your affiant believes these envelopes contained the cash from each retail locations' sales. Moreover, your affiant has not seen check disbursements from the bank accounts of the Defendants' Companies that appear sufficient to constitute the full wages of Unlimited employees. In addition to not seeing the payments in the

banking records, your affiant has reviewed Maryland wage records for several quarters, which reported wages for very few Unlimited employees.

44. The electronic messages about the employees' wages are also revealing in other ways. For example, your affiant located one message sent on or about December 27, 2015 that shows the large number of people that were being paid. The first names listed in this message correspond, with some spelling variations, to the first names of the 51 people from the employee list sent to **A. SHARVIT** on or about December 20, 2015 (excepting M.S., I.A., I.A.#2, and N.G.). The paycheck list also indicates whether the employee had provided customers with refunds.

45. Your affiant believes that **O. SHARVIT** functioned as a manager who was responsible for day-to-day functions associated with the cosmetics sales businesses including directing and managing employees. He participated in WhatsApp messages about the recruitment of foreign citizens in Israel to work for Unlimited, the assignment of employees, visa extensions, and setting the daily schedule.

46. On or about May 12, 2015, **O. SHARVIT** wrote in a WhatsApp message in English asking co-conspirator #2 needed to confirm "that the company in Israel don't [sic] tell to the new employees that they finish their day at 8:00 pm" and to "bring me me [sic] maximum of employees bcse [sic] we are going to conquest America!!!!" Your affiant believes "the company in Israel" refers to the recruiting company used by the Defendants in Israel.

47. **O. SHARVIT** also played a role in the termination of employees. For example, on or about December 29, 2015, **O. SHARVIT** sent a message to other Defendants and co-

conspirators stating “[first name of E.S.¹⁷] is fired. Please prepare his paycheck of the last week, he's leaving Tomorrow morning.” In December 2015, E.S. was in the United States on a B-2 visitor visa. He departed the United States on or about January 6, 2016.

48. On or about January 4, 2016, **O. SHARVIT** sent a WhatsApp message to other Defendants and co-conspirators stating: “[First name of M.G.¹⁸] needs visa extension emergency, Shes burnt [sic] tomorrow!” Your affiant believes this referred to M.G. and that “burnt” meant she would be a visa overstay. This conclusion is based on context and on a check of government records which show that M.G. was granted a period of admission to the U.S. as a B-2 visitor that ended on or about January 8, 2016.

49. On or about December 26, 2016, **O. SHARVIT** sent a WhatsApp message stating in part “[nickname of A.B.] burned in two weeks. Working til 1/1/17 . visa extension refused, [co-conspirator #3] will check again the papers with him tomorrow night. He already talked with Rona about it. I continue siha with him tomorrow. (Possible to convince him to stay and find somebody to marry).” Your affiant believes “siha” might be a reference to meetings from the context. Your affiant believes “Rona” refers to **ZHFANI** and submits that this message demonstrates that **O. SHARVIT** knew and understood the unlawful purpose of the conspiracy, in particular, how the Defendants were using commission-based, illegal labor to operate their businesses by purposely circumventing the United States visa and immigration process. He was

¹⁷ There is a one letter variation in the first name of the employee between the message and the employee list sent on or about December 20, 2015, one uses a “y” and the other an “i.”

¹⁸ There is a one letter variation in the first name of the employee between the message and the employee list sent on or about December 20, 2015, one uses a single “a” and the other uses two, e.g. “aa.”

even willing to go further, as demonstrated here by the seeming reference to a potential marriage fraud to allow an Unlimited employee to remain in the United States.

50. Your affiant believes that **ZHFANI** held a similar position in the company to **O. SHARVIT**. She also functioned as a manager who was responsible for helping to set schedules, assigning employees to housing, and managing employees.

51. On or about June 12, 2015, **ZHFANI** sent a WhatsApp message to other Defendants and co-conspirators containing a list of approximately 8 apartments and approximately 27 first names assigned to the apartments. On or about September 29, 2015, **ZHFANI** sent a WhatsApp message to other Defendants and co-conspirators containing a list of approximately 9 apartments and approximately 30 first names. On or about November 21, 2015, **ZHFANI** sent a WhatsApp message to other Defendants and co-conspirators containing a list of approximately 12 apartments and approximately 42 first names. Based on the investigation, your affiant believes these names were employees working for Defendants' Companies and living in housing provided by the companies.

52. On or about March 8, 2016, **ZHFANI** sent a WhatsApp message directly to co-conspirator #1. Based on your affiant's use of Google Translate the message appears to state, in part, as follows: "Tell Oren to close the girl and the guy they are not connected to that company are in another company that is afraid now after this story and decided to make all their employees legal !! They're going to be monsters here!" Your affiant submits that "Oren" refers to **O. SHARVIT** and that in this message **ZHFANI** is discussing recruiting workers for Unlimited and that her reference to "employees legal" refers to using employees who could be legally employed in the United States.

53. On or about October 18, 2016, **ZHFANI**, other Defendants, and co-conspirators

received a WhatsApp message that contained a PDF file with the airline boarding passes of three foreign citizens, S.L., E.E., and Y.G. In a response that your affiant Google translated, **ZHFANI** responded by asking if they had a phone and whether there was a photo of the employees to help locate them. U.S. government databases reveal that S.L., E.E., and Y.G. entered the U.S. on or about October 19, 2016 on B-2 visitor status. Records also show that S.L. and E.E. interviewed for their U.S. visas together and were issued B-1/B-2 visas on or about October 5, 2016.

54. On or about October 21, 2016, **ZHFANI** sent a message to other Defendants and co-conspirators, which your affiant used Google to translate, stating that [first names of S.L. and E.E.] had been assigned rooms.

There Is Probable Cause To Believe The Target Accounts Contain Relevant Evidence

55. As detailed throughout this affidavit, your affiant and other federal agents have obtained evidence revealing **A. SHARVIT** and **ZHFANI**'s extensive use of electronic devices in furtherance of the crimes under investigation, in particular, WhatsApp messages and, in the case of **A. SHARVIT**, emails¹⁹. The Defendants used electronic messaging to carry out their criminal activities, including to exchange business information with each other and other co-

¹⁹ Based on information obtained pursuant to an email search warrant for an account associated to **A. SHARVIT** your affiant receipt Internet Protocol ("IP") address information for IP addresses used to access the account. Your affiant input those IP addresses into an internet service used to lookup more details on an IP address (<https://www.ultratools.com/tools/ipWhoisLookupResult>) and found that on or about January 29, 2018, February 6, 2018, February 7, 2018, February 11, 2018, February 14, 2018, and February 15, 2018 the email account was accessed from IP addresses that the internet search tool shows belong to AT&T Mobility LLC. Your affiant knows that as of in or about August 2017, the phone number linked to **A. SHARVIT** in the WhatsApp messages was serviced by AT&T. Your affiant submits that it is likely that these IP addresses indicate that he accessed his email from a cellular device.

conspirators such as employee work schedules, pay amounts due to employees, and visa extension information.

56. Based on information uncovered to date in the investigation, there is probable cause to believe that **A. SHARVIT**, **O. SHARIVT**, and **ZHFANI** all used smartphones and have sent WhatsApp messages²⁰ about the conspiracy from 2015-2017 and that **A. SHARVIT** has sent emails about Defendants' Companies and that **ZHFANI** has posted relevant photographs to Facebook.²¹

57. Your affiant has learned from a government individual that if an iPhone user has an AppleID and signs in with it on an iPhone then the iPhone, by default, is set to back-up data from the iPhone, unless the user changes the backup settings. This data is backed up to the iCloud linked to the AppleID. Based on this, your affiant submits there is probable cause to

²⁰ Based on my experience, your affiant know that WhatsApp messages are stored on the device used to send or receive the messages. Therefore, unless deleted, **A. SHARVIT** and **ZHFANI**'s devices contain copies of the incriminating messages outlined herein.

²¹ On the publicly visible portion of **ZHFANI**'s Facebook page, your affiant found pictures of foreign citizens who your affiant believes based on the investigation have worked for the Defendants' Companies. Your affiant reviewed the photos on **ZHFANI**'s Facebook page and found one group title "iOS Photos" and another "Mobile Uploads" which your affiant understands refers to photos uploaded from Apple devices and mobile devices respectively. Within those albums, your affiant located photos of a BioXage store and photos of people standing in front of a Deja Vu kiosk. The albums also contained many photos of **ZHFANI** photos of others including some photos that had been tagged to other Facebook accounts including the accounts matching the names of S.Y., Y.E., M.G.#2, R.Z., and A.B. – all five were named on an employee list sent to **A. SHARVIT** on or about December 20, 2015 and all five filed visa extensions linked to the fraud scheme. Based on my knowledge and experience, your affiant knows that a photograph is often saved on a user's device before it is uploaded to Facebook. Therefore, there is probable cause to believe that at lease some Facebook photos are likely stored on **ZHFANI**'s personal electronic device(s).

believe that any iCloud data stored on accounts with Apple IDs linked to the IMEI of the phones of **A. SHARVIT** and **ZHFANI** likely contain additional relevant electronic evidence.

INFORMATION REGARDING APPLE ID AND iCloud²²

58. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

59. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

²² The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “iCloud: iCloud storage and backup overview,” available at <https://support.apple.com/kb/PH12519>; and “iOS Security,” available at https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

60. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

61. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

62. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

63. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

64. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is

linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

65. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user’s instant messages on iCloud.

66. Your affiants believes that evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

67. For example, the stored communications contained on an iCloud backup connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

68. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information and iCloud logs may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the use and user of the accounts during events relating to the crime under investigation.

69. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

70. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, emails and instant messages from the iCloud back-up, can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

71. Therefore, Apple's servers are likely to contain iCloud back-ups which contain stored iCloud back-ups and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

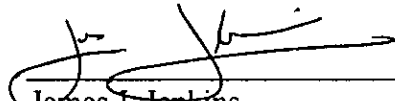
72. Your affiant seeks this search warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), which permits this Court to issue a search warrant requiring Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) described with particularity in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

18 - 2691 - ADC

73. Based on the forgoing, I request that the Court issue the proposed search warrant.

This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,


James J. Jenkins
Special Agent,
Diplomatic Security Service
Department of State

Subscribed and sworn to before me on 2 October, 2018


A. DAVID COPPERTHITE
UNITED STATES MAGISTRATE JUDGE

18 - 2691 - ADC

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the APPLE IDs (the "Target Accounts") associated/linked with the following International Mobile Equipment Identities ("IMEI"):

1. IMEI 356572082018670; and

2. IMEI 353841087910253

which are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ps

18 - 2691 - ADC

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages),

HA

18 - 2691 - ADC

My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

f. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

g. All records pertaining to the types of service used; and

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

18 - 2691 - ADC

II. Information to be seized by the government

For the time period January 1, 2013 to the present, all information described above in Section I relating to violations of violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1546 (visa fraud), 18 U.S.C. §§ 1512(k), 1519 (obstruction of justice), 8 U.S.C. § 1324 (harboring aliens), and 8 U.S.C. § 1324a (unlawful employment of aliens):

1. All electronic data, documents, records, and information regarding (a) citizens of other countries entering, remaining in, or leaving the United States; (b) the hours, compensation, duties, location, supervision, job performance, logistics, immigration status, recruitment of, or contracting with foreign workers; (c) the travel, transportation, and housing of any foreign citizen; (d) the hiring, hours, payroll, payment of, period of employment, firing, qualifications or background of any employee of any business with locations in the United States; (e) the consideration of, the preparation for, the payment for, or an application to extend a U.S. visa including related documents and correspondence; (f) information provided to or submitted to the U.S. Citizen and Immigration Services, U.S. Customs and Border Protection, Immigration Customs Enforcement, the U.S. Department of Homeland Security, or the U.S. Department of State; and (g) all current, former, or future employees of businesses associated in any way with the following individuals or entities: Mordehay (aka Moti) FOOX, Asher SHARVIT (aka CHARBIT), Rona ZHFANI (aka SHARVIT), Oren SHARVIT (aka CHARBIT), Eyal CHERTOFF, Esti (aka Esty) MAZOR (collectively "Defendants"), Unlimited Treasures, Unlimited 13, Deja Vu, BioXage, BH Distribution Group LLC, 3505 Clarks Ln LLC, and/or Filicori Zecchini (collectively "Defendants' Companies").
2. All electronic data, documents, records, and information regarding communications and financial arrangements with aliens and foreign citizens, and the employment and use of aliens and foreign citizens.
3. All electronic data, documents, records, and information regarding the finances and business interests of the Defendants or the Defendants' Companies.
4. All electronic data, documents, records, and information relating to the U.S. immigration laws, and the submission of information to U.S. or state authorities.
5. All electronic data reflecting attempts to obstruct justice, including but not limited to the destruction of documents and electronic evidence, and attempts to corruptly persuade co-conspirators and witnesses with regard to any investigations into the Defendants' crimes.
6. All electronic data, documents, records, and information regarding financial transactions, assets, and the transfers of things of value, including bank statements, wire transfer records,

loan records, credit card records, ledgers, checks or other monetary instruments, check registers, lines of credit, and safe deposit box keys and records.

7. Any and all electronic data, documents, records, and information constituting or relating to any personal or corporate income tax return and the supporting schedules and attachments to include but not limited to Internal Revenue Service Forms 1120, 1120s, 941, 940, 1040, 1040ez, W-2, 1099, K-1 and schedules such as Schedule C, E and related tax information
8. All data, records, and information regarding the use of the device(s) backed up to the Target Accounts to communicate with other individuals, including but not limited to:
 - a. All telephone numbers and direct connect numbers assigned to the device, including usernames and passwords and electronic mail addresses;
 - b. All call and direct connect history information;
 - c. All contacts and associated telephone numbers;
 - d. All stored electronic mail, including attachments; and
 - e. All voice recordings, videos, text messages, messages in applications, and other messages stored on the phone.
9. All electronic data, records, and information regarding the following:
 - a. Contact information, phone numbers, mailing addresses, email addresses, calendars, datebooks, domains, or other contact information for any of the individuals, addresses, or entities listed herein;
 - b. Calendar information;
 - c. Stored photographs, videos, and text messages;
 - d. Stored documents and other files;
 - e. Stored geo-location information;
 - f. Data stored in any application;
 - g. The times the device or a device function was used;
 - h. Evidence of the attachment to the device of other storage devices or similar
 - i. containers for electronic evidence;
10. All electronic data, records, and information regarding the use of the device backed up to the Target Accounts to connect to the internet and/or connect with other cellular or computer devices, including but not limited to:
 - a. All information about Internet Protocol addresses accessed by the device;
 - b. All information about the Internet Protocol addresses of any entities/persons accessing the device; and
 - c. All web-browsing history and any stored web pages.
11. All electronic data, showing who used or owned the devices backed up to the Target Accounts at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history.

18 - 2691 - ADC

12. Any and all electronic data and information that would tend to show the identity of the person using the device backed up to the Target Accounts.
13. Evidence of user attribution showing who used or owned the devices backed up to the Target Accounts at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, phone numbers, saved user names and passwords, documents, browsing history, email, email contacts, "chats," instant messaging logs, photographs, and correspondence;
14. The identity of the person(s) who created or used the Target Accounts, including records that help reveal the whereabouts of such person(s);
15. Evidence indicating how and when the Target Accounts were accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber; and
16. Any records pertaining to the means and source of payment for services associated with the Target Accounts (including any credit card or bank account number or digital money transfer account information).